WINDOWS RED TEAM OPERATOR

Malware Analysis & Development w/t Practical & Hands-On

Adversary Simulation & C2 Frameworks

RED TEAM : C2 Frameworks

C2 frameworks — the abbreviation to the ***Command and Control (C&C) infrastructure*** — are how red teamers and pentesters can control compromised machines during security assessments.

- Although implemented on other models (P2P or out of band), C2 frameworks are typically designed under a client-server architecture and used to communicate with systems via a network connection.
- These kinds of systems mimic benign network traffic to avoid detection and bypass network security appliances.
- Many techniques can be used to establish command and control based on different levels of stealth depending on the victim's network, structure, and defenses (MITRE ATT&CK).

In detail, MITRE presents 16 distinct C2 techniques grouped into several sub-techniques and observed in past cyber incidents. (*visit+)

RED TEAM : C2 Frameworks

Usually, when an initial foothold is established, that point can move laterally through the internal network, using the C2 capabilities and jumping to other vulnerable or misconfigured network points.

- As expected, the first compromised machine is a ***valuable target***.
- It is typically used as a pivot to access more sensitive network parts such as file servers and domain controllers.

As C2 is a bi-directional application, sensitive information can be easily exfiltrated from the environment.

- In the last few months, several cyberattacks were registered with a lot of stolen sensitive data, from military documents to credit cards and PII.
- To finish the chain, criminals can efficiently deploy data encryption malware such as ransomware via C2 to extort their victims.

RED TEAM : C2 Frameworks

Mostly used C2 post-exploitation frameworks during RED Teaming & internal assessments:

- **Cobaltstrike**
- **Covenant**
- **Sillenttrinity**
- **Koadic**
- **Metasploit**
- **Merlin**
- **Many More**

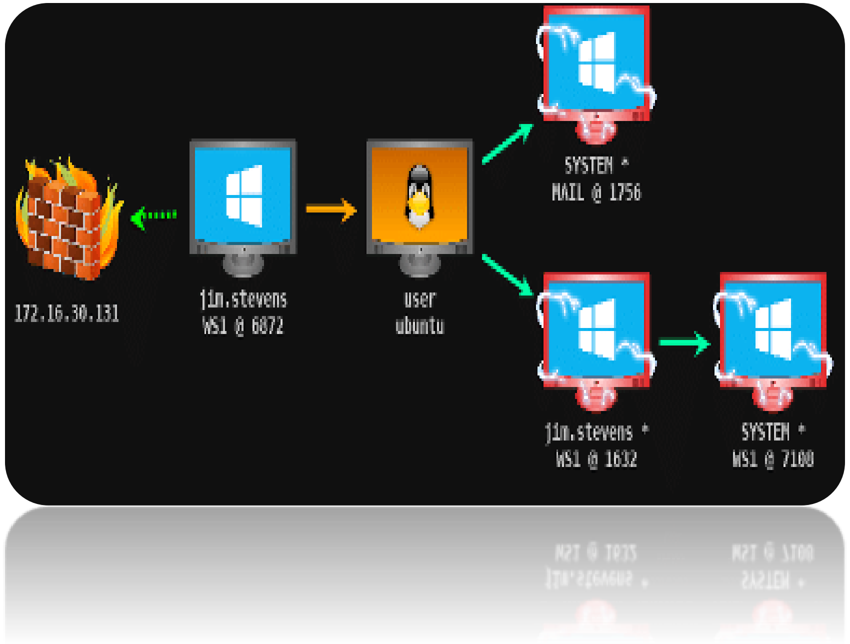
C2 Frameworks: 1st Cobalt Strike (Link)

Cobaltstrike is one of the most used platforms worldwide that is mainly used for Adversary Simulations and Red Team Operations.

URL: https://www.cobaltstrike.com/

Cobaltstrike is one of the most used platforms worldwide that allows the deployment of a beacon agent on the victim’s machine.

- This kind of agent provides a lot of functionalities, including:



Keylogging, file upload and download, socks proxy, VPN deployment, privilege escalation techniques, Mimikatz, port scanning and the most advanced lateral movements.

C2 Frameworks: 1st Cobalt Strike (Link)

- The Cobaltstrike beacon uses a file-less approach under a stageless or multistage shellcode typically loaded by exploring a vulnerability or a weakness that will execute in memory the final payload without touching the disk.
- It supports C2 connection via HTTP, HTTPS, DNS and SMB protocols.
- In addition, Cobaltstrike also provides a development toolkit called

  Artifact Kit that facilitates customized shellcode loaders.

C2 Frameworks: 1st Cobalt Strike (Link)

- The Cobaltstrike beacon uses a file-less approach under a stageless or multistage shellcode typically loaded by exploring a vulnerability or a weakness that will execute in memory the final payload without touching the disk.
- It supports C2 connection via HTTP, HTTPS, DNS and SMB protocols.
- In addition, Cobaltstrike also provides a development toolkit called

  Artifact Kit that facilitates customized shellcode loaders.

C2 Frameworks: 2nd Covenant (Link)

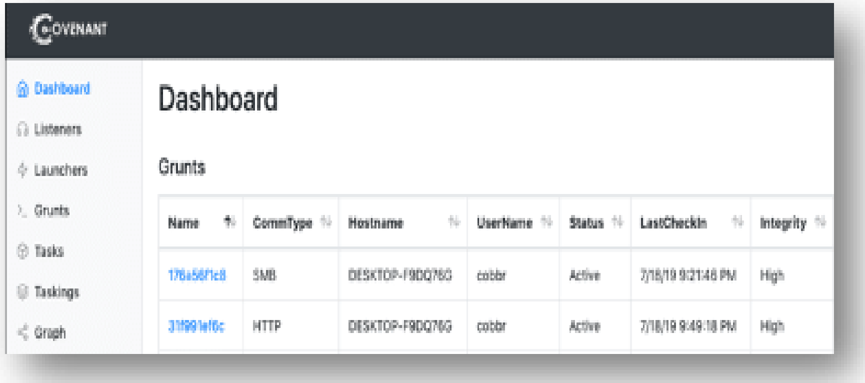
Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers.

- Is an ASP.NET Core, cross-platform application that includes a web-based interface that allows for multi-user collaboration.

Key Features:

- **Intuitive Interface** - provides an intuitive web application to easily run a collaborative red team operation.
- **Multi-Platform** - targets .NET Core, which is multi-platform. This allows Covenant to run natively on Linux, MacOS, and Windows platforms. Additionally, Covenant has Docker support, allowing it to run within a container on any system that has Docker installed.
- **Multi-User** - supports multi-user collaboration. The ability to collaborate has become crucial for effective red team operations. Many users can interact with the same Covenant server and operate independently or collaboratively.
- **API Driven** - Is driven by an API that enables multi-user collaboration and is easily extendible.

C2 Frameworks: 2nd Covenant (Link)



Dashboard

Grunts

Name	CommType	Hostname	UserName	Status	LastCheckIn	Integrity
176a56f1c8	SMB	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:21:46 PM	High
31f991ef6c	HTTP	DESKTOP-F9DQ76G	cobbr	Active	7/18/19 9:49:18 PM	High

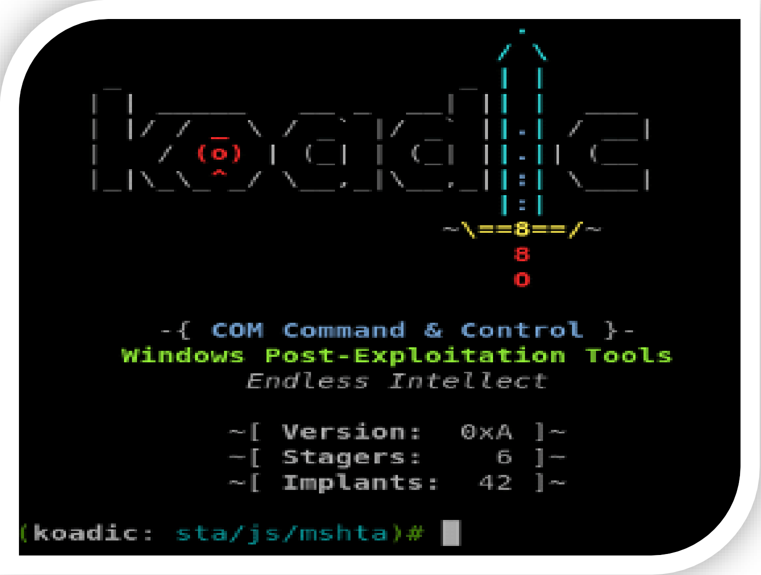
- **Developed in C#** - It is nice to have all components of framework written in the same language.
- **Listener Profiles** - supports listener “profiles” that control how the network communication between Grunt implants and Covenant listeners look on the wire.
- **Encrypted Key Exchange** - Implements an encrypted key exchange between Grunt implants and Covenant listeners, in addition to optional SSL encryption. This achieves the cryptographic property of forward secrecy between Grunt implants.
- **Dynamic Compilation** - Uses the Roslyn API for dynamic C# compilation. Every time a new Grunt is generated or a new task is assigned, the relevant code is recompiled and obfuscated with ConfuserEx, avoiding totally static payloads.
- **Inline C# Execution** – Allows operators to execute C# one-liners on Grunt implants.
- **Tracking Indicators** - Tracks “indicators” throughout an operation, and summarizes them in the Indicators menu. This allows an operator to conduct actions that are tracked throughout an operation and easily summarize those actions to the blue team during or at the end of an assessment for deconfliction and educational purposes.

C2 Frameworks: 3rd Sillenttrinity (Link)

- Sillenttrinity is an asynchronous and multi-server C2 framework developed in Python3 and .NET DLR.
- This platform uses embedded third-party .NET scripting languages and dynamically calls .NET APIs; the author entitled BYOI (Bring Your Own Interpreter) technique.
- This tool uses a dedicated team server with many modern features into a powerful C2 framework.
- The usage of WebSockets allows effective real-time communication between the team server and the agents installed on the victims' machines.
- It uses Ephemeral Elliptic Curve Diffie-Hellman Key Exchange to encrypt all C2 traffic between the team server and its implant.
- One of the appreciated features is its modularity — users can modify any module easily.

C2 Frameworks: 4th Koadic (Link)

- Koadic is a Windows post-exploitation framework that uses Windows Script Host (JScript/VBScript) and supports all Windows versions from Windows 2000 to Windows 11.
- This framework is written in Python, and its payloads are JavaScript-based with XOR encryption.
- The agents are installed on the target machines using the default mshta or using the default mshta or Microsoft HTML Application stagers.
- Is an open-source tool and is available on GitHub.



```
          -{ COM Command & Control }-
        Windows Post-Exploitation Tools
               Endless Intellect

            ~[ Version:  0xA ]~
            ~[ Stagers:    6 ]~
            ~[ Implants:  42 ]~

(koadic: sta/js/mshta)#
```

C2 Frameworks: 5th Metasploit (Link)

- The Metasploit framework is a popular tool distributed along with Kali Linux distribution and can be used to find vulnerabilities on networks and servers.
- As it is an open-source tool, it can be customized by operators and used with many operating systems, including Android, iOS, macOS, Linux, Windows, Solaris, etc.
- Meterpreter is equipped with many features, including staged and non-staged payloads to enable port forwarding between networks.

C2 Frameworks: 6th MERLIN (Link)

- Merlin is a C2 that uses HTTP/1.1, HTTP/2 and HTTP/3 protocols to evade detection and communicate with its agents.
- Merlin is a cross-platform tool written in Golang and capable of working in several operating systems.
- Each merlin compilation will generate unique payloads capable of avoiding AV detection from the detection point-of-view.
- It uses a client-server architecture and provides the most advanced features of red teaming presented on other C2 frameworks in the market.
- As it is an open-source project, operators can customize Merlin agents, their *modus operandi* and how it is loaded into the memory.

C2 Frameworks: 7th BlackMamba (Link)

- Black Mamba is a Command and Control (C2) that works with multiple connections at same time.
- Developed with Python and with Qt Framework and have multiples features for a post-exploitation step.

Some Features

- Multiple clients.
- Real-time communication.
- Encrypted communication
- Screenshot gathering.
- Real-time video capture.
- Locking of client mouse.
- Download and upload of files.
- Keylogger.
- Web downloader.

https://github.com/loseys/BlackMamba

C2 Frameworks: 8th EMPIRE (Link)

- Empire 4 is a post-exploitation framework that includes a pure-PowerShell Windows agents, Python 3.x Linux/OS X agents, and C# agents.
- It is the merger of the previous PowerShell Empire and Python EmPyre projects.
- The framework offers cryptologically-secure communications and flexible architecture.

- On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework.

https://github.com/BC-SECURITY/Empire

C2 Frameworks: 9th Starkiller (Link)

- Starkiller is a Frontend for Powershell Empire.
- It is an Electron application written in VueJS.

Key Features:

- Interactive agent shell
- Malleable profile management
- Enable/Disable modules
- Process Browser
- File browser
- Popout windows
- Chat widget
- Bypass management

https://github.com/BC-SECURITY/Starkiller

https://www.bc-security.org/post/an-introduction-to-starkiller

C2 Frameworks: 10th NORTHSTAR C2 (Link)

- An open-source C2 framework developed for penetration testing and red teaming purposes.
- Consists of two applications, a server-side GUI web application for managing sessions and a client-side stager to communicate with C2 server.

Features

- **Languages and technologies used in the NorthStar C2**:
  Client-Side: C # .NET & ***Server-Side:*** PHP, JS, HTML, CSS

Client-side application (**NorthStar Stager**) has the following functions:

- Connecting to the C2 Server via HTTP or HTTPS,
- Receiving commands from the server-side application & responding to the command via HTTP methods,
- Encrypting the communication traffic with XOR and obfuscating it with Base64,
- Persistence through start-up folders and schtasks,
- Host Reconnaissance : Hostname, Username, Current Privileges, Exec Dir and Process ID,

https://github.com/EnginDemirbilek/NorthStarC2

C2 Frameworks: 10th NORTHSTAR C2 (Link)

- Privilege Escalation : UAC bypass through eventvwr.exe,
- Taking screenshots and saving them into a directory,
- Uploading any file to the victim machine,
- Downloading any file from the victim machine,
- SAM dump via reg save command,
- Changing the working directory,
- View the files and folders in the directory,
- Viewing the contents of the files,
- Deleting files,
- Send commands directly on cmd.exe.

Server-side application has the following functions:

- User-Friendly GUI with everything needed to manage sessions opened by the stager.

https://github.com/EnginDemirbilek/NorthStarC2

Practical - LAB
Open Source C2 Frameworks:
Installations & Working

Additional Resources:

Remote Access Tools

Cobalt Strike is software for Adversary Simulations and Red Team Operations. https://cobaltstrike.com/

Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. https://github.com/EmpireProject/Empire

Metasploit Framework is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. https://github.com/rapid7/metasploit-framework

SILENTTRINITY A post-exploitation agent powered by Python, IronPython, C#/.NET. https://github.com/byt3bl33d3r/SILENTTRINITY

Pupy is an opensource, cross-platform (Windows, Linux, OSX, Android) remote administration and post-exploitation tool mainly written in python. https://github.com/n1nj4sec/pupy

Koadic or COM Command & Control, is a Windows post-exploitation rootkit similar to other penetration testing tools such as Meterpreter and Powershell Empire. https://github.com/zerosum0x0/koadic

PoshC2 is a proxy aware C2 framework written completely in PowerShell to aid penetration testers with red teaming, post-exploitation and lateral movement. https://github.com/nettitude/PoshC2_Python

Additional Resources:

Gcat a stealthy Python based backdoor that uses Gmail as a command and control server. https://github.com/byt3bl33d3r/gcat

TrevorC2 is a legitimate website (browsable) that tunnels client/server communications for covert command execution. https://github.com/trustedsec/trevorc2

Merlin is a cross-platform post-exploitation HTTP/2 Command & Control server and agent written in golang. https://github.com/Ne0nd0g/merlin

Quasar is a fast and light-weight remote administration tool coded in C#. Providing high stability and an easy-to-use user interface, Quasar is the perfect remote administration solution for you. https://github.com/quasar/QuasarRAT

Covenant is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive .NET tradecraft easier, and serve as a collaborative command and control platform for red teamers. https://github.com/cobbr/Covenant

FactionC2 is a C2 framework which use websockets based API that allows for interacting with agents and transports. https://github.com/FactionC2/

DNScat2 is a tool is designed to create an encrypted command-and-control (C&C) channel over the DNS protocol. https://github.com/iagox86/dnscat2

Sliver is a general purpose cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. https://github.com/BishopFox/sliver

EggShell is a post exploitation surveillance tool written in Python. It gives you a command line session with extra functionality between you and a target machine. https://github.com/neoneggplant/EggShell